Lecture 2

§2.0. Recall: last time we defined G/H as a set, for any subgroup H of a group G. We proved that for H normal subgroup, G/H naturally carries a group structure such that the natural projection $\pi : G \longrightarrow G/H$ is a group homomorphism.

For today G will be assumed to be finite, unless I explicitly make an assertion about infinite groups [finite: as a set]. $|G| = \#$ of elements in G is called order of G.

e.g. $|S_n| = n!$ $\quad |\mathbb{Z}/_{N\mathbb{Z}}| = N.$

§2.1. Let $H < G$ be a subgroup. Then G breaks into disjoint union of left cosets

$$G = \bigsqcup_{\alpha \in A} g_\alpha H$$

union is over a choice of representatives of their respective equivalence class (recall $x \sim y$ if $x^{-1}y \in H$ - this equivalence rel^{n} was used in the defn of G/H).

So A is in bijection with G/H. Hence we obtain the first counting lemma:

Lemma. $|G| = |H| \cdot |G/H|$

(for a proof we only need to observe that $|gH| = |H|$ for any $g \in G$).

Cor. $|H|$ divides $|G|$.

Rk. $|G/H|$ is usually denoted by $(G:H)$ - index of H in G. It is possible for G and H to be infinite and yet $(G:H) < \infty$.

e.g. $\left.\begin{array}{l} G = \mathbb{Z} \\ H = 5 \cdot \mathbb{Z} \end{array}\right\}$ are infinite $(G:H) = 5 < \infty$.

In this case we say H is a subgroup of finite index.

§ 2.2. Let $a \in G$. By <u>order of a</u> we mean the smallest positive integer k such that $a^k = e$. In this case $H = \langle a \rangle$ (subgp. generated by a) is of order k and hence by Corollary from § 2.1 above, k divides $|G|$.

<u>Remark.</u> If G is infinite, no such k need to exist. In that case we will say <u>a is of infinite order</u>.

§ 2.3. Groups acting on sets.

Let G be a (not necessarily finite) group and X a set. By an action of G on X we mean a set map

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto g \cdot x$$

(this will be a <u>left</u> action)

such that

(i) $e \cdot x = x \quad \forall\, x \in X$

(ii) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x \quad \forall\, g_1, g_2 \in G,\ x \in X$

Given G acting on X, we get, $\forall g \in G$, a set map

$$\tau(g) : X \longrightarrow X$$
$$x \longmapsto g \cdot x$$

- $\tau(e) = \mathrm{Id}_X$
- $\tau(g) \circ \tau(g^{-1}) = \tau(e) = \mathrm{Id}_X$

  $\Rightarrow$ each $\tau(g)$ is a bijection
- $\tau(g_1) \circ \tau(g_2) = \tau(g_1 g_2)$

In simpler terms, $\tau : G \longrightarrow \mathrm{Aut}(X)$ $\left(= \{ \underbrace{f : X \to X}_{\text{bijection}} \} \right)$ is a group homomorphism.

§2.4. More vocabulary.

- I personally use the notation $G \circlearrowright X$ (read: G acts on X)
- $G \circlearrowright X$ is <u>faithful</u> if $\tau : G \longrightarrow \mathrm{Aut}(X)$ is injective
- $G \circlearrowright X$ is <u>transitive</u> if $\forall x, y \in X$, $\exists g \in G$ s.t. $g \cdot x = y$.
- $G \circlearrowright X$ is <u>free</u> if $\forall x \in X$, $[g \cdot x = x \Rightarrow g = e]$.

- For $x \in X$, the orbit (in X) of x, denoted by

$$Gx := \{g \cdot x : g \in G\} \quad \left(= \{y \in X \text{ s.t. } \exists\, g \in G \text{ with } g \cdot x = y\}\right)$$

- Stabilizer of x (in G) is:

$$\operatorname{Stab}_G(x) := \{g \in G : g \cdot x = x\}$$ (sometimes also denoted by G_x ← in subscript)

- The set of orbits (or G-orbits) in X is denoted by $G \backslash X$.

[Note: $\forall\, x, y \in X$, either $G \cdot x = G \cdot y$
or $G \cdot x \cap G \cdot y = \phi$]

We have the following analogue of Lemma 2.1 (p. 2)

Lemma. (a) $$|G| = |G \cdot x| \, |\operatorname{Stab}(x)| \quad (\forall\, x \in X)$$

(b) $$|X| = \sum_{\alpha \in G \backslash X} \frac{|G|}{|\operatorname{Stab}(x_\alpha)|}$$

(here $x_\alpha \in X$ is a choice of an element from the G-orbit labelled by $\alpha \in G \backslash X$).

Proof. (a) Let $x \in X$. Define $\phi : G \to G\cdot x$

$$g \mapsto g\cdot x$$

By definition ϕ is surjective.

$$\phi(g_1) = \phi(g_2) \iff g_1 \cdot x = g_2 \cdot x$$

$$\iff g_1^{-1} g_2 \cdot x = x \quad (\text{i.e. } g_1^{-1} g_2 \in \mathrm{Stab}(x))$$

$\Rightarrow$ we have a bijection $G/_{\mathrm{Stab}(x)} \to G\cdot x$

and (a) follows.

(b) Break X into disjoint union of G-orbits

$$X = \bigsqcup_{\alpha \in G\backslash X} G\cdot x_\alpha$$

$$\Rightarrow |X| = \sum_{\alpha \in G\backslash X} |G\cdot x_\alpha| \underset{\text{by (a)}}{=} \sum_{\alpha \in X\backslash G} \frac{|G|}{|\mathrm{Stab}(x_\alpha)|}$$

$\square$

§ 2.5. Some examples

(1) $G = S_n \circlearrowright \{1, \ldots, n\}$

Faithful	T	F
Transitive	T	F
Free	T	F

$\leftarrow \mathrm{Stab}_{S_n}(n) = S_{n-1}$.

(2) $$G = \left\{ \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} : 0 \leq \theta \leq 2\pi \right\}$$

$G \circlearrowright \mathbb{R}^2 \setminus \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$

Faithful	T	F
Transitive	T	F
Free	T	F

(3) $G \circlearrowright G/H$ by $g \cdot (g'H) = (gg')H$

Faithful ? Transitive ? Free ? (Exercise)

§ 2.6. Burnside's Counting Lemma.

$G \circlearrowright X$. Let $g \in G$ and define

Set of fixed points of g $\longrightarrow$ $X^g := \{ x \in X : g \cdot x = x \}$

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Proof. Let $F = \{(g,x)\in G\times X : g\cdot x = x\}$

- Sum over 1^{st} component

$$|F| = \sum_{g\in G}|X^g|$$

- Sum over 2^{nd} component

$$|F| = \sum_{x\in X}|\operatorname{Stab}(x)|$$

So
$$\sum_{g\in G}|X^g| = \sum_{x\in X}|\operatorname{Stab}(x)| = \sum_{\alpha\in G\backslash X}\sum_{x_\alpha\in\alpha}|\operatorname{Stab}(x_\alpha)|$$

$$= \sum_{\alpha\in G\backslash X}|G|\cdot\sum_{x_\alpha\in\alpha}\frac{1}{|G\cdot x_\alpha|}$$ (by (a) of Lemma (2.4) page 5)

$$= |G|\cdot\sum_{\alpha\in G\backslash X}1$$

$$= |G|\cdot|G\backslash X|$$ $\square$